Basic Cybersecurity Training for Fermilab Visitors

Cybersecurity is everyone's responsibility!

Why is cybersecurity training important?

- Fermilab is a government entity; all devices on the Fermilab network are tempting targets for attackers.
- A **single** individual's careless or unknowing action can cause significant harm to the entire laboratory.
- Cybersecurity is a partnership between the Cybersecurity Team (CST), lab management, users.
- As a Fermilab visitor, **YOU** are a user and a part of this partnership.
- **Your specific role:** accountable for the machines you have on the Fermi network.
- You must complete this training to obtain/renew your visitor badge.

Social engineering

- Social engineering is the process of tricking someone into disclosing personal information (such as username/password), or running malicious code on their computer.

- This is typically accomplished via **phishing emails** that are designed to look like real emails to lure you into clicking on a malicious link.

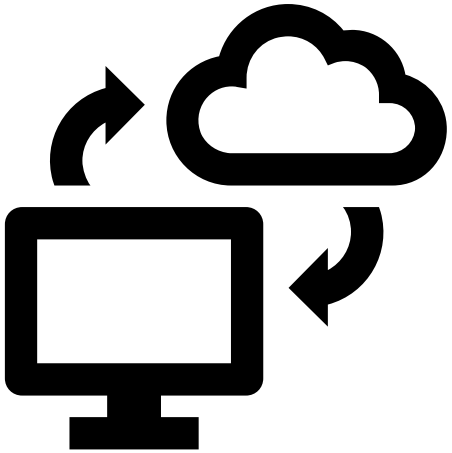
Signs of phishing emails to watch for:

- Emails that require immediate action or create a sense of urgency.
- Emails with generic salutations.
- Grammar or spelling mistakes.

Actions to take when you suspect phishing:

- Hover mouse over the links.
- Copy URLs from email to browser.
- Only open attachments you were expecting.
- Call and confirm if a friend/colleague sent the message.

Safe web browsing



- Web browsing is a primary contributor of malware. This occurs when legitimate websites have been compromised to redirect you to another site controlled by hackers.
- If you get a malware infection from visiting a site running malicious code, this is referred to as a **drive-by download.**

- **Practice safe web browsing habits with the following:**
  - Be careful when browsing!
  - Use an ad-blocker such as uBlock Origin.
  - **NEVER browse the web with an admin account.**
  - Only run up-to-date web browsers with up-to-date web components.
  - Run anti-virus with up-to-date virus signatures.

Physical security

- If an attacker gains physical access to your computer, it is effectively compromised because anything can be done to the machine at that point.

- **Maintaining physical security is easy:**
  - Always lock your screen when away from the computer.
    - Windows: Windows Key + L
    - Mac: Control + Command Q
  - Use a different password for every account, including SERVICES, FERMI, and Kerberos.
    More information: https://cd-docdb.fnal.gov/cgi-bin/sso/RetrieveFile?docid=3172&filename=AuthenticationPolicy.pdf&version=7
  - Do not leave unattended laptops in visible areas such as on a desk or in your car.
  - Machines in unlocked/common areas should use a cable lock to prevent theft.
  - Lock your office door at the end of the day if possible.

Policy highlights

- **Appropriate Use of Laboratory Computers and Fermilab Network**
  - Laboratory computers—or any devices on the laboratory network—should be used for laboratory business. Limited incidental use consistent with the Fermilab Policy on Computing on Prohibited Activities is allowed.
  - All computer users are required to behave in a way that maintains the security of the laboratory's computing environment.

- **Prohibited Use Of Laboratory Computers/Networks**
  - Illegal activities or activities that offend other employees or users or result in the embarrassment to the lab.
  - Uploading, downloading, viewing or storing sexually explicit material.
  - Uploading or downloading copyrighted material.
  - Using unlicensed software.
  - Activities in support of an ongoing private business.
  - Activities that consume excessive computing resources (disk space, network bandwidth, etc.).
  - Having unpatched or outdated devices on the network.
  - Bypassing Fermilab security controls.

-Reporting-

You must promptly report any actual, or even suspected, security breaches or incidents 24 x 7 to the Service Desk at x2345, or email the Cybersecurity Team at: cybersecurity@fnal.gov.

Detailed rules are provided in the Fermilab Policy on Computing.

Congratulations!

You have completed Basic Cybersecurity Training for Fermilab Visitors.

Please enter the following code on your Visitor Request Form to indicate that you have completed this training:

FermiCyber2019